



COMSATS Institute of Information Technology, Abbottabad
Department of Computer Science

Course: CSC 432 – Telecom Network Design (3,0)
(Spring 2015)

Office: Z-Block (Z-359)
Instructor: Rab Nawaz Jadoon
(Assistant Professor)
Office hours: (9.00 am to 5.00 pm)
Email: rabnawaz@ciit.net.pk

Course Objectives

- Develop an understanding of how mission objectives and mission requirements generate network service and network design requirements.
- Understand the need for network analysis and how network analysis contributes to the development of User Requirements Documents and network design.
- Understand the elements of structured network design process.
- Understand the logical design process for core, distribution, and access networks, and how logical network design processes contribute to the development of User Requirements Documents.
- Understand the importance of host and network address allocation and naming plans in the network design processes.
- Understand how switching and routing requirements influence network design decisions.
- Understand network security and network management strategies influence network designs.
- Understand the elements of the physical design process for access, distribution, and core networks.
- Understand how network services allocation and provisioning contribute to network design decisions.

Required Text Books

- Top Down Network Design (2nd Edition), Priscilla Oppenheimer, Cisco Press, 2004.
ISBN 1-58705-152-4
- Network Analysis, Architecture, and Design (3rd Edition), James McCabe, Morgan Kaufmann Publishers, 2007. ISBN 978-0-12-370480-1

Lectures Handouts:

For **Course Related Updates** kindly visit the following link,

<https://jadoon956.wordpress.com/networks/>

Part I → Network Analysis

1. Analyzing Business Goals and Constraints

- Using a Structured Network Design Process
- Systems Development Life Cycles
- Plan Design Implement Operate Optimize (PDIOO) Network Life Cycle
- Analyzing Business Goals
- Working with Your Client
- Changes in Enterprise Networks
- Networks Must Make Business Sense
- Business Goals Checklist

2. Analyzing Technical Goals and Tradeoffs

- Scalability
- Planning for Expansion
- Expanding Access to Data
- Constraints on Scalability
- Availability
- Disaster Recovery
- Specifying Availability Requirements
- Five Nines Availability
- The Cost of Downtime
- Network Performance
- Network Performance Definitions
- Optimum Network Utilization
- Throughput
- Throughput of Internetworking Devices
- Accuracy
- Efficiency
- Manageability
- Usability
- Adaptability
- Affordability
- Making Network Design Tradeoffs
- Technical Goals Checklist

3. Characterizing the Existing Internetwork

- Characterizing the Network Infrastructure
- Developing a Network Map
- Characterizing Large Internetworks
- Characterizing the Logical Architecture
- Characterizing Network Addressing and Naming
- Characterizing Wiring and Media
- Checking Architectural and Environmental Constraints
- Checking a Site for a Wireless Installation
- Performing a Wireless Site Survey
- Checking the Health of the Existing Internetwork
- Developing a Baseline of Network Performance
- Analyzing Network Availability
- Analyzing Network Utilization

- Measuring Bandwidth Utilization by Protocol
- Analyzing Network Accuracy
- Analyzing Errors on Switched Ethernet Networks
- Analyzing Network Efficiency
- Analyzing Delay and Response Time
- Checking the Status of Major Routers, Switches, and Firewalls
- Network Health Checklist

4. Characterizing Network Traffic

- Characterizing Traffic Flow
- Identifying Major Traffic Sources and Stores
- Documenting Traffic Flow on the Existing Network
- Characterizing Types of Traffic Flow for New Network Applications
- Terminal/Host Traffic Flow
- Client/Server Traffic Flow
- Peer-to-Peer Traffic Flow
- Server/Server Traffic Flow
- Distributed Computing Traffic Flow
- Traffic Flow in Voice over IP Networks
- Characterizing Traffic Load
- Calculating Theoretical Traffic Load
- Refining Estimates of Traffic Load Caused by Applications
- Estimating Traffic Load Caused by Routing Protocols
- Characterizing Traffic Behavior
- Broadcast/Multicast Behavior
- Network Efficiency
- Network Traffic Checklist

Part II → Logical Network Design

5. Designing a Network Topology

- Hierarchical Network Design
- Why Use a Hierarchical Network Design Model?
- Flat Versus Hierarchical Topologies
- Flat WAN Topologies
- Flat LAN Topologies
- Mesh Versus Hierarchical-Mesh Topologies
- Classic Three-Layer Hierarchical Model
- Core Layer
- Distribution Layer
- Access Layer
- Guidelines for Hierarchical Network Design
- Redundant Network Design Topologies
- Backup Paths
- Load Sharing
- Modular Network Design
- Cisco SAFE Security Reference Architecture
- Designing a Campus Network Design Topology
- Virtual LANs

- Fundamental VLAN Designs
- Wireless LANs
- Positioning an Access Point for Maximum Coverage
- WLANs and VLANs
- Redundant Wireless Access Points
- Redundancy and Load Sharing in Wired LANs
- Server Redundancy
- Workstation-to-Router Redundancy
- Gateway Load Balancing Protocol
- Designing the Enterprise Edge Topology
- Redundant WAN Segments
- Circuit Diversity
- Multihoming the Internet Connection
- Virtual Private Networking
- Site-to-Site VPNs
- Remote-Access VPNs
- Service Provider Edge
- Secure Network Design Topologies
- Planning for Physical Security
- Meeting Security Goals with Firewall Topologies

6. Designing Models for Addressing and Numbering

- Guidelines for Assigning Network Layer Addresses
- Using a Structured Model for Network Layer Addressing
- Administering Addresses by a Central Authority
- Distributing Authority for Addressing
- Using Dynamic Addressing for End Systems
- IP Dynamic Addressing
- Zero Configuration Networking
- Using Private Addresses in an IP Environment
- Caveats with Private Addressing
- Network Address Translation
- Using a Hierarchical Model for Assigning Addresses
- Why Use a Hierarchical Model for Addressing and Routing?
- Hierarchical Routing

7. Selecting Switching and Routing Protocols

- Making Decisions as Part of the Top-Down Network Design Process
- Selecting Switching Protocols
- Switching and the OSI Layers
- Transparent Bridging
- Selecting Routing Protocols
- Characterizing Routing Protocols
- Distance-Vector Routing Protocols
- Link-State Routing Protocols
- Routing Protocol Metrics
- Hierarchical Versus Nonhierarchical Routing Protocols
- Interior Versus Exterior Routing Protocols
- Classful Versus Classless Routing Protocols
- Dynamic Versus Static and Default Routing
- On-Demand Routing

- Scalability Constraints for Routing Protocols
- Routing Protocol Convergence
- IP Routing
- Routing Information Protocol
- Enhanced Interior Gateway Routing Protocol
- Open Shortest Path First
- Intermediate System-to-Intermediate System
- Border Gateway Protocol
- Using Multiple Routing Protocols in an Internetwork
- Routing Protocols and the Hierarchical Design Model
- Redistribution Between Routing Protocols
- Integrated Routing and Bridging
- A Summary of Routing Protocols

8. Developing Network Security Strategies

- Network Security Design
- Identifying Network Assets
- Analyzing Security Risks
- Analyzing Security Requirements and Tradeoffs
- Developing a Security Plan
- Developing a Security Policy
- Components of a Security Policy
- Developing Security Procedures
- Maintaining Security
- Security Mechanisms
- Physical Security
- Authentication
- Authorization
- Accounting (Auditing)
- Data Encryption
- Public/Private Key Encryption
- Packet Filters
- Firewalls
- Intrusion Detection and Prevention Systems
- Modularizing Security Design

Part III → Physical Network Design

9. Selecting Technologies and Devices for Campus Networks

- LAN Cabling Plant Design
- Cabling Topologies
- Building-Cabling Topologies
- Campus-Cabling Topologies
- Types of Cables
- LAN Technologies
- Ethernet Basics
- Selecting Internetworking Devices for a Campus Network Design
- Criteria for Selecting Campus Internetworking Devices
- Optimization Features on Campus Internetworking Devices

- Example of a Campus Network Design
- Technical Goals
- Network Applications
- User Communities
- Data Stores (Servers)

10. Selecting Technologies and Devices for Enterprise Networks

- Remote-Access Technologies
- Password Authentication Protocol and Challenge Handshake
- Authentication Protocol

Evaluation methods

Assignment/Quizzes → 25%

First Sessional → 10%

Second Sessional → 15%

Final Term → 50%

Rules and policy in this class

1. Although the rules and policy defined here may seem a little bit rush, they are not meant to cause any harm to you instead to protect you and to prepare you for better life and to become professionals.
2. Students are not allowed to bring their family members for day care or baby sitting. The classroom is not a place for children.
3. Student behavior/classroom decorum: “Free discussion, inquiry, and expression are encouraged this class.” However, classroom behavior that interferes with either the instructor’s ability to conduct the classroom or the ability of students to benefit from the instruction is not acceptable.
4. Please turn off (or place on silence) your beepers and cellular phones before the lecture starts. In the event of a situation where student legitimately needs to carry a beeper/cellular telephone to class, prior notice and approval of the instructor is required.
5. No use of electronic devices while in class unless required or approved by the instructor.
6. Classroom behavior which is deemed inappropriate and cannot be resolved by the student and the faculty member may be referred to the Office of DCO, 1st Floor C-Block; telephone (851), for administrative or disciplinary review as per the code of Students Conduct.
7. As part of the academic integrity outlined in the current General Catalogue: “Students are expected to maintain the highest standards of academic integrity. Behavior that violates these standards is not acceptable.
8. Students are NOT allowed to share their assignments and to communicate during the tests or exam.
9. No student is allowed in the class if not officially registered in this class.

10. Late assignment will be penalized as follow after the assignment due date and time: 10% off the first day, 25% off the second day, 50% off the third day, and “Zero” after that. All the assignments will be due in class on the specified due date.
11. No makeup test or exam will be given except in the case of emergency such as the student being sick and he/she is unable to come to class in which case an official Doctor’s excuse MUST be presented to the instructor. The student concerned is required to take the make up test/exam no later than two lectures or class periods after he/she returns to class. Failure to comply will result in the grade of zero (0) for the test/exam.
12. All students are encouraged to attend class and on time. I will be taking rolls randomly. A total of five (6) absences will result in the grade of “F” in this class for the student(s) concerned.
13. It is totally forbidden to voice or/and video record this course lecture presentations without a written agreement signed and dated between the student and the instructor. Any violation to this rule will result to the invasion of the instructor privacy.
14. Finally, I am totally open to any constructive critics or/and suggestions.

Emergency Evacuation

In the case of fire or emergency, please do not panic and simply follow your instructor’s emergency procedure evacuations.